Langley Research Center

LPR 1740.4

Effective Date: July 22, 2004

Expiration Date: March 6, 2008

FACILITY SYSTEM SAFETY ANALYSIS AND CONFIGURATION MANAGEMENT

National Aeronautics and Space Administration

RESPONSIBLE OFFICE: OFFICE OF SAFETY AND MISSION ASSURANCE

PREFACE

This Langley Procedural Requirements (LPR) sets forth procedural requirements for the Langley Research Center (LaRC) System Safety and Configuration Management (CM) Programs for the Center's ground-based research facilities. It defines the requirements of the Center's Facility System Safety Analysis and CM Programs. It also provides guidance for government personnel in performing their responsibilities for these programs.

LAPG 1740.4, dated July 24, 2002, is rescinded and should be destroyed.

Delma C. Freeman, Jr.
Deputy Director

DISTRIBUTION:
SDL 040, SDL 043, SDL 4 1 0, SDL 41 1, and SDL 412
429/OSMA (150 copies)

TABLE OF CONTENTS

TABLE OF CONTENTS (Cont.)

Chapter **Page**

APPENDICES

Appendix **Page**

LIST OF FIGURES

Page

RECORDS

NASA Langley Form 127, Change Notification Sheet
NASA Langley Form 129, Change in Laboratory Equipment/Procedures (CLEP).
Safety analysis documentation
Standard Operating Procedures
Checklist
Safety Analysis Report
Configuration controlled documentation
Engineering drawing files
Pressure Systems Configuration Management Revision Record
Laboratory Risk Evaluation Revision Record
Asbestos Configuration Management Reports

REFERENCES

LAPD 1700.2, Safety Assignments
LAPD 7000.2, Review Program for Langley Research Center (LaRC) Facility Projects
LPR 1710.42, Safety Program for Maintenance of Ground-Based Pressure Vessels and Pressurized Systems
LPR 1740.2, Facility Safety Requirements
LPR 1740.7, Process Systems Certification Program
LMS-CP-4710, Configuration Management for Facilities
LMS-CP-4890, Construction and Change Assurance for High Risk Facilities
LMS-CP-5528, Software Planning, Development, Acquisition, Maintenance, and Operation
LMS-CP-5529, Software Configuration Management Planning for Low-, High-, and Critical-Control Software
NASA Langley Form 127, Change Notification Sheet
NASA Langley Form 129, Change in Laboratory Equipment/Procedures (CLEP).

Chapter 1

1. FACILITY SYSTEM SAFETY PROGRAM

1.1 INTRODUCTION

The LaRC Facility System Safety Program exists to ensure the safe and continuous operation of ground-based LaRC facilities. It is comprised of two major components: safety analysis and configuration management. A safety analysis takes the form of either a Facility System Safety Analysis or Laboratory Risk Analysis. LaRC's configuration management programs are as follows:

- Facility Configuration Management (CM) Program,
- Pressure Systems Configuration Management (PSCM),
- Software Configuration Management (SCM),
- Laboratory Risk Evaluation Program (LREP), and
- Asbestos Configuration Management Program (ACMP).

LaRC facilities included in the Facility CM Program have been designated as high-risk and have had a safety analysis conducted in accordance with the Facility System Safety Analysis process. The Safety Manager shall appoint an Office of Safety and Facility Assurance (OSFA) Safety Engineer to be the safety point of contact for each of these facilities. Each facility also has a unique number, called an Effort Code (EC), to aid in tracking configuration controlled documentation (CCD). The present high-risk facilities and their EC number are listed in Figure 1-1, "Effort Code Summary." Most research facilities not in the Facility CM Program are included in the LREP, which provides for both safety analysis and configuration management.

Whether a research facility/equipment is placed in the Facility CM Program or LREP depends on the complexity and/or risk associated with its operation. The OSFA shall decide whether a research facility or piece of research equipment is placed in the Facility CM Program or LREP. Items that are either commercially available or not a complex system/facility (i.e., a small vacuum chamber) represents typical items placed in the LREP. Complex, high-risk facilities are placed in the Facility CM Program. These are facilities that need to be divided into systems/subsystems to facilitate the safety analysis.

Details on the Facility System Safety Analysis process, LREP, and the various CM programs are found in the remainder of this document as described below:

- **Chapter 2** addresses the Facility System Safety Analysis process,
- **Chapter 3** addresses the Facility CM Program,
- **Chapter 4** addresses the PSCM Program,
- **Chapter 5** addresses the SCM Program,
- **Chapter 6** addresses the LREP, and
- **Chapter 7** addresses the ACMP.

EC	FACILITY NAME
01	High Pressure Air System
02	Hypersonic CF_4 Tunnel
03	8-Foot High Temperature Tunnel
04	1- X 3-Foot High Enthalpy Aerothermal Tunnel
05	Hypersonic Blowdown Tunnels (8): • 20” Mach 6 Tunnel • Nozzle Test Chamber • 12” Mach 6 High Reynolds Number Tunnel • Gas Mixing Apparatus • 18” Mach 8 Tunnel • 1/2 Meter Quiet Tunnel • 20” Supersonic Wind Tunnel • Probe Calibration Tunnel
07	Hypersonic N^2 Tunnel
12	Entry Structures Facility
13	Visual Motion Simulator
14	Drive Control
16	31-Inch Mach 10 Tunnel
17	15-Inch Mach 6 High Temperature Tunnel
18	Transonic Dynamics Tunnel
19	14- X 22-Foot Subsonic Tunnel
21	16-Foot Transonic Tunnel
22	Aircraft Noise Reduction Laboratory
23	Hypersonic Materials Test Apparatus
24	Unitary Wind Tunnel
25	Scramjet Test Facility
26	High Reynolds Number Helium Tunnel Complex
27	High Reynolds Number Helium Recovery System
28	Hypersonic Helium Tunnel Facility
29	Aircraft Landing Dynamics Facility
31	Vortex Research Facility
33	Impact Dynamics Research Facility
34	0.3-Meter Transonic Cryogenic Tunnel
35	Anechoic Noise Facility
36	Jet Noise Apparatus
37	Thermal Acoustic Fatigue Apparatus
40	Low Turbulence Pressure Tunnel
50	Vacuum Sphere Control and 60-Foot Space Simulator
55	Cockpit Motion Facility
58	Impact and Projectile Range
61	12-Foot Low Speed Tunnel
62	20-Foot Vertical Spin Tunnel
64	DC-9 Simulator
65	Visual Landing Display System
66	Differential Maneuvering Simulator
67	General Purpose Fighter Simulator
68	General Aviation Simulator
69	7-Inch High Temperature Tunnel
71	Vitiated Heater, Test Cell #2
75	Combined Loads Test System (COLTS) – Test Machine
76	Combined Loads Test System (COLTS) – Cryobox
80	Combustion and Mixing Research Apparatus, Test Cell #1
84	Hangar Water Deluge System
85	Heavy-Duty Brazing Vacuum Furnace
86	16-Meter Thermal Vacuum Chamber
89	Autoclaves
91	Composite Shop Autoclave
92	Hypersonic Helium Tunnel Recovery System
93	Transport Systems Research Vehicle (TRSV)
97	Space Systems Structures Research Laboratory
98	Steam Distribution System
99	National Transonic Facility (NTF)

Figure 1-1, Effort Code Summary.

1.2 OBJECTIVES

The objectives of LaRC's Facility System Safety Program are:

- Ensure that the appropriate safety analysis has been conducted,
- Ensure that designated facilities/systems are placed under the appropriate level of configuration management, and
- Document risk and provide the information to management and operating personnel.

The objectives of a safety analysis, whether a Facility System Safety Analysis or Laboratory Risk Evaluation, are:

B. Identify credible hazards,
C. Define the hazards in terms of severity and probability,
D. Assess the controls for those hazards, and
E. Make recommendations toward reduction of the severity and/or probability of occurrence.

Both the Facility CM Program and the LREP:

- Record and maintain safety analysis documentation,
- Document and maintain standard operating procedures for use by operating personnel, and
- Ensure the OSFA reviews changes that affect safety.

In addition, the Facility CM Program establishes and maintains a baseline for designated systems (e.g., electrical systems) and the relevant documentation (e.g., drawings).

LaRC's PSCM and ACMP are special CM programs. The objective of the PSCM is to maintain the configuration of Pressure System Documents (PSD); these are documents that provide detailed information about a particular high pressure system. The objectives of the ACMP are: (1) increase safety awareness and minimize the risk of asbestos exposure to personnel and (2) institute controls to prevent the release of asbestos fibers, restrict future asbestos use, and develop surveillance and control of known, existing asbestos applications in LaRC facilities.

1.3 DEFINITIONS

The glossary at Appendix A lists and defines the terms unique to the Facility System Safety and CM Programs.

Chapter 2

2. FACILITY SYSTEM SAFETY ANALYSIS

2.1 PROGRAM SUMMARY

A Facility Systems Safety Analysis (FSSA) is a systematic approach toward:

- Identifying credible hazards associated with the operation of a facility,
- Defining the hazards in terms of severity and probability,
- Assessing the controls for those hazards,
- Making recommendations toward reduction of the severity and/or probability of occurrence, and
- Identifying documentation to place under configuration control.

A FSSA shall be performed prior to the start of research activities at a new facility, prior to the start of research activities at an existing facility that has undergone a Construction of Facility (CoF) modification, or prior to any existing facility being brought into the Facility CM Program. The final documents of this effort, all of which shall be placed in the Facility CM Program, are

- Standard Operating Procedures (SOP's) and Checklists,
- Safety Analysis Report (SAR),
- Configuration Control Documentation (CCD),
- Other special items identified by the Facility Team.

The SAR documents the results of the FSSA. The remaining items support the FSSA and ensure hazard controls (e.g., procedures, interlocks, etc.) have been documented and placed under configuration control. This ensures the long term safe operation of the facility.

The overall responsibility for conducting the FSSA lies with the Office of Safety and Facility Assurance (OSFA), Office of Safety and Mission Assurance (OSMA). However, the analysis is a group effort conducted by a Facility Team. A Facility Team includes:

- Organizational Facility Safety Head (OSFA) (henceforth called FSH),
- Facility Coordinator (FC),
- Facilities Configuration Coordinator (FCC) from the Systems Engineering Competency (SEC),
- Safety Engineer from OSFA, and
- Safety Engineer from the Recertification and Configuration Management (R&CM) contractor or other.

The above members of a Facility Team are permanent members who also assist with meeting the requirements of the Facility CM Program. For new facilities or CoF projects, the Technical Project Engineer (TPE) from the SEC is also a member of the Facility Team during performance of the FSSA.

2.2 PLANNING AND EXECUTION

For an existing facility that will be added to the Facility CM Program, the assigned OSFA Safety Engineer will notify the responsible FSH approximately 60 days prior to initiation of a FSSA. The FSH, with the assistance of the facility staff and technicians, will assemble and provide to the OSFA Safety Engineer all existing documentation that reflects the “as-is" facility configuration. These documents include:

- The appropriate facility electrical and mechanical drawings (redlined if necessary);
- Draft SOP’s and/or checklists;
- Vendor manuals, maintenance plans and engineering reports/analyses; and
- Any other item that may be of value toward the system safety analysis such as operational logs, failure mode histories, and specific areas of concern.

These documents form the foundation of the Safety Engineer's formal analysis of the facility's hazards and other conditions appropriate to the issue of safety. Details of how to develop a SAR, SOP’s, and identify CCD are discussed in the following paragraphs.

For new facilities or CoF projects, it is very important that the OSFA Safety Engineer be involved during all phase of design, construction, and shakedown. For these projects, the FSSA shall be an integral part of the design process as outlines in Section 3.4.4, “Change Controlled by Design Review Process.” At the start of any new project, the TPE or FSH shall contact the OSFA Safety Engineer, who shall initiate the FSSA.

2.3 SOP’S AND CHECKLISTS

Instructions for the development of SOP’s and Checklists are found in the following paragraphs. Facility complexity and operational risks dictate the requirement for the degree of structured operations, which shall be controlled by SOP’s and/or Checklists.

2.3.1 SOP Guidelines

SOP’s are detailed, written, formal instructions for qualified operators to use during operation of the facility. The basic guidelines to be followed in the preparation of SOP’s are listed below.

- SOP’s shall provide for a complete cycle of operation (dormant to run back to dormant). This cycle will be presented in three separate sections: Pre-Operational Procedures (PR), Operational Procedures (OP), and Post-Operational Procedures (PO).
- SOP’s shall be designed to alert operators of potentially unexpected events. These alerts shall be expressed in three distinct categories:
    - **NOTES.** General instruction to the operator concerning the specific order that procedures must follow. They alert the operator to potential undesired

events of a minor nature (that is, failure to comply would invalidate previous actions), and they provide explanatory information.
  - **CAUTIONS.** Specific alerts to the operator that the sequence, which follows, could cause equipment damage if not executed as specified.
  - **WARNINGS.** Specific alerts to the operator that the sequence, which follows, could cause personnel injury or death if not executed as specified.
- SOP's for the complete cycle shall be demonstrated and approved prior to being included in the CM Program.
- Initially, demonstrations shall be "dry runs" to avoid unnecessary exposure to hazards.
- SOP's shall be approved by the preparer, reviewer, Safety Manager and FSH.
- SOP's shall be placed under configuration control in accordance with the requirements of Chapter 3.

2.3.2 Checklist Guidelines

Checklists are abbreviated versions of SOP's and are intended to provide less-detailed instructions for routine, day-to-day operation of a facility by experienced personnel. Checklists are not required for a facility in the CM Program. However, if a facility chooses to have checklists they must be demonstrated, approved, and brought under CM prior to their use. The developmental process shall be identical to that followed in the development and approval of SOP's. Some guidelines to be used in their preparation are listed below.

- A Checklist may cover an entire cycle of operation or any part thereof; however, it must be clearly labeled as to what it covers.
- A Checklist may be of a "check off" or "sign off" nature, or it may be simply a sequential listing of steps to be taken without the need to check/sign items off.
- A Checklist is often reproduced within the facility and a copy used for each operational run. In such cases, the entire Checklist must be reproduced and no part of the original omitted.

2.3.3 SOP/Checklist Organization

SOP's/Checklists will be divided into two sections: Introductory Matter and Text.

2.3.3.1 Introductory Matter

The Introductory Matter consist of the Title Page, Revision Record, and General Introduction.

The **Title Page** contains the SOP/Checklist title, the name of the facility for which the document was completed, and the facility number in which the facility is housed.

The **Revision Record** reflects all SOP/Checklist document changes as well as who prepared, reviewed, and accepted those changes. These shall be:

- The "Prepared By" column shall be signed by the person who prepared the change.

- The "Reviewed By" column shall be signed by the designated reviewing authority.
- The "Reviewed By Safety Manager" column shall be signed by the Safety Manager.
- The "FSH Cognizance" column shall be signed by the FSH.

A **General Introduction** page addresses the purpose, personnel, support and safety services, equipment, initial conditions, and reference drawings appropriate to the procedures/checklist being presented.

2.3.3.2 Text

The Text section begins immediately following the Introductory Matter and consists of a Sequence Flow Chart, which shows the safe order in which the preoperational (PR), operational (OP), and postoperational (PO) procedures can be executed, followed by the actual, step-by-step SOP/checklist.

2.3.4 SOP's/Checklists Changes and Distribution

Since SOP's/Checklists are CCD's, they shall be changed and distributed in accordance with the requirements set fourth in Chapter 3 of this document.

2.4 SAFETY ANALYSIS REPORTS (SAR's)

A SAR is the formal documentation of the FSSA and shall be prepared in accordance with Section 2.4.2. It shall be a CCD document and any change to the facility will be considered for possible SAR impact.

2.4.1 SAR Organization

The SAR is divided into three main sections — Introductory Matter, Text, and Appendices. The Text is further subdivided into subsections common to all facilities although, on a case-by-case basis, additional special-item subsections (for example, a CIL) can be added. The common subsections of the Text are the Introduction, the Facility Description and the Safety Analysis Summary. The following is a discussion of each section.

2.4.1.1 Introductory Matter

The Introductory Matter consists of the Title Page, Revision Record, List of Page Revisions, and Table of Contents.

The **Title Page** contains the report title, the name of the facility for which the report was completed, the building number in which the facility is housed, and the Effort Code (EC) associated with the facility.

The **Revision Record** reflects all changes to a SAR; who prepared, reviewed, and accepted the report/changes; and the date issued. The required signatures are as follows:

- The “Prepared By" column shall be signed by the Safety Engineer who prepared the report/change.
- The “Reviewed By" column shall be signed by the designated reviewing authority.
- The “Reviewed By Safety Manager" column shall be signed by the Safety Manager.
- “FSH Cognizance” column shall be signed by the FSH.

The **Table of Contents** lists the major subsections of the SAR and the page number on which each begins.

2.4.1.2 Text

The Text section of the SAR consists of the Introduction, the Facility Description, and the Safety Analysis Summary.

The **Introduction** identifies the facility, states the purpose and philosophy of the analysis, and explains the Risk Assessment logic.

The **Facility Description** provides a brief overview of the subject facility and describes the major facility capabilities, the nature of research conducted, the subsystems, and any special facility features appropriate to the safety analysis. It also includes a Facility Block Diagram that shows the general relationships among the various subsystems.

The **Safety Analysis Summary** contains two sections: General Observations & Recommendations and Tabular Summary. General Observations and Recommendations address the Hazards that are general in scope as opposed to specific to a particular subsystem and documents any other fact the Safety Engineer feels is relevant to the SAR but does not belong in an Appendix. The Tabular Summary subsection lists and discusses the identified Undesired Events and the associated risks. The Tabular Summary presents a synopsis of the Safety Analysis of each major subsystem, which is given in detail in the appendices. Each Hazard/Undesired Event shall be assigned an alphanumeric Risk Level in accordance with the philosophy and guidelines established in Section 2.4.4.

2.4.1.3 Appendices

The appendices of the SAR provide a detailed discussion of the Hazards, Undesired Events, and Risk Assessments. There is a separate appendix for each major subsystem identified on the Facility Block Diagram.

2.4.1.4 Critical Items List (CIL)

The SAR includes a Critical Items List (CIL) for any facility that has a Critical Item. A Critical Item is any item, the single order failure of which would likely result in death or damage to equipment/property equal to or greater than $1.0M. Section 2.4.2 provides more details about preparing a CIL.

2.4.1.5 SAR Changes and Distribution

Since SOP's/Checklists are CCD's, they shall be changed and distributed in accordance with the requirements set fourth in Chapter 3 of this document.

2.4.2 SAR Preparation

The Safety Manager shall appoint an OSFA Safety Engineer to be responsible for the preparation of a SAR. The actual preparation is performed by either the OSFA Safety Engineer or a Safety Engineer from a support contractor. Any SAR prepared by a support contractor shall be reviewed and approved by the OSFA Safety Engineer.

The following definitions provide a uniform understanding of the terms related to SAR preparation:

- **Hazard.** A condition which has the potential to result in damage to equipment and/or personnel injury/death.
- **Undesired Event.** An event (or series of events) which unleashes the potential inherent in a hazard, and either directly or indirectly results in equipment damage and/or personnel injury/death.
- **Cause.** The stimulus or triggering mechanism/act which precipitates the Undesired Event.
- **Effect.** The consequence of the Undesired Event in terms of equipment damage and/or personnel injury/death.

2.4.2.1 Phases

The phases of SAR preparation is outlined in Figure 2-1, "SAR Preparation Sequence." A description of each phase follows.

The first phase is the **System Definition Phase**. During this phase, the Safety Engineer uses facility provided documentation to define the system. The facility is divided into manageable subsystems. Examples of such subsystems are high pressure air, vacuum, model injection, cooling water, test section, nitrogen, hydrogen, and so forth. How these subsystems are identified in any given facility depends on the methodology used by the Safety Engineer in organizing the SAR to cover every aspect of the facility. For example, in one instance, the model injection component may be a separate subsystem; whereas, in another instance, it may be included as part of the test section subsystem. The important thing is to ensure that all components of the facility are analyzed. Also at this time, a Facility Block Diagram is generated to show the interrelationships among the chosen subsystems.

Next, the Safety Engineer performs a **Preliminary Hazard Analysis (PHA)** to identify all the possible Hazards and the Undesired Events that could result from those Hazards. This phase represents an initial safety assessment of the facility. The Hazards and Undesired Events established here will be expanded as the safety analysis progresses. There may be none or any number of Hazards in each of the subsystems. Upon completion of this phase, copies of the products will be sent to the Facility Team for initial review and clarification of the facility Hazards and Undesired Events.

Upon completion of the PHA the **Initial Facility Team Review** is conducted. The Facility Team conducts an initial review of the effort by examining the System Definition and Preliminary Hazard Analysis products and provides the Safety Engineer additional information and comments.

With input from the Facility Team, the Safety Engineer performs a **Detailed Hazard Analysis (HA).** The HA ensures that a deductive approach is taken in the assessment of the safety implications of the facility and it documents that thought process. The approach that to be taken is reflected in Figure 2-1. Details of how to perform a HA are provided in Section 2.4.3.

With the subsystems, Hazards, and Undesired Events defined, the Safety Engineer prepares a **Critical Items List (CIL)**, if required. A Critical Item is any item, the single order failure of which would likely result in death or damage to equipment/property equal to or greater than $1.0M. A Critical Item must have the design analyses, in-service inspection/preventive maintenance procedures, installation procedures, and nondestructive testing required to establish and maintain an acceptable probability of occurrence. The requirement for design calculations can be waived for Critical Items which are proprietary or part of a company's standard product line providing that the item has been designed to industry consensus codes, a history of acceptable operations of the same or similar products is available, and the use is in compliance with the manufacturer's ratings and recommended applications. Examples of proprietary items that meet the design waiver criteria are large rotating machinery for wind-tunnel compressor or drive systems. Critical Items listed in a SAR shall be tracked throughout their lifetime for compliance with design, maintenance, and inspection requirements. Pressure components that are standard product lines and built to national consensus codes or standards are not considered Critical Items. However, these items are covered under LaRC’s Pressure System Recertification Program to assure system integrity.

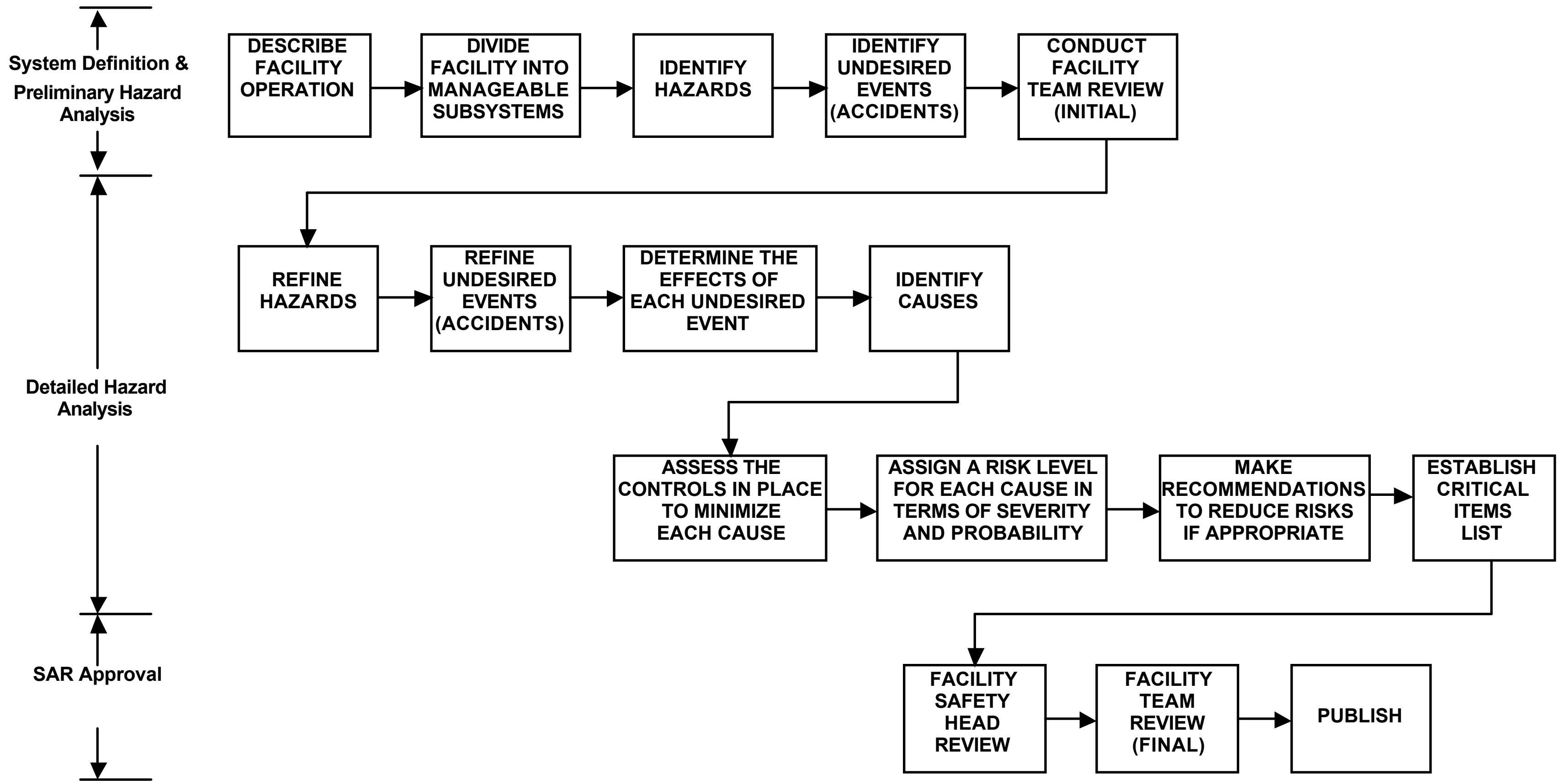

Figure 2-1, SAR Preparation Sequence.

At this point, a complete SAR is ready for a **Facility Safety Head Review.** The FSH conducts a thorough and independent review of the SAR.

Once the Safety Engineer and FSH agree that the SAR is complete a **Final Facility Team Review** is conducted. During this phase, the remaining members of the Facility Team review the SAR.

Finally, the SAR is **Published.** After all of the issues are resolved and the SAR is prepared in final format, it shall be formally approved by the Safety Manager and FSH. Finally, it shall be incorporated into the CM Program.

2.4.3 Hazard Analysis

The HA begins with a detailed exploration of each of the identified Hazards (an example of one might be hot surfaces). Considering that Hazard, the Safety Engineer establishes what event(s) could occur that would result in the Hazard causing damage, injury, and/or death (for example, personnel in contact with hot surfaces). Those events become the Undesired Events. There could be multiple Undesired Events resulting from each identified Hazard. The analyst then quantifies the Effects of each Undesired Event in terms of damage, injury, and/or death (for example, serious injury to personnel). When numerous effects result, only the most severe is noted.

Next, the Safety Engineer establishes what could cause an Undesired Event to occur, and these become the Causes (for example, personnel error). There could be one or multiple causes for the same Undesired Event. To determine a facility's ability to avoid the occurrence of an Undesired Event, the Safety Engineer assess the safety devices and procedures that minimize the probability of occurrence of each Cause. This assessment takes the form of an investigation of the design and operational features that reduce the probability of each individual Cause from occurring.

In the interest of plausibility, the Undesired Events, Causes, and Effects are to be confined to “credible" as opposed to “conceivable" events. They should reflect only those things that could reasonably be expected to occur.

The next step in the analysis is the Risk Assessment. An individual assessment is made and a Risk Assessment Code (RAC) assigned to each of the identified Causes using the guidance provided in Section 2.4.4. If an assigned Risk Assessment is unacceptable, as outlined in Section 2.4.4, recommendations are made, which would reduce that Risk Assessment to acceptable limits if implemented. These recommendations can take the form of additional safety devices, design changes, or changes in the SOP.

HAZARD SEVERITY

The Hazard Severity Categories provide a relative measure of the worst possible consequences resulting from personal error, environmental conditions, design inadequacies, procedural deficiencies, or system or component failure/malfunction, with no consideration being given to abatement techniques. They are:

CATEGORY I - CATASTROPHIC. May cause death, permanent disability, the hospitalization of three or more people, and/or system/equipment damage in excess of $250,000 (Type A or B mishap).

CATEGORY II - CRITICAL. May cause loss time injury or illness, and/or system/equipment damage between $25,000 and $250,000 (Type C mishap).

CATEGORY III - MARGINAL. May cause minor injury or illness, and/or system/equipment damage between $1000 and $25,000 (Reportable incident).

CATEGORY IV - NEGLIGIBLE. Will not result in injury, illness, or system/equipment damage in excess of $1000 (Nonreportable incident).

HAZARD PROBABILITY

Hazard probability is the likelihood that a hazard will occur during the planned life expectancy of the system. The probability level is quantitative, based on engineering judgment, with appropriate guidelines as follows.

LEVEL A - FREQUENT. The level assigned when neither a safety feature nor approved procedures exist to prevent the Undesired Event from occurring.

LEVEL B - OCCASIONAL. The level assigned when a safety feature does not exist, but the use of approved procedures should prevent the Undesired Event from occurring.

LEVEL C - POSSIBLE. The level assigned when approved procedures do not exist, but an existing safety feature should prevent the Undesired Event from occurring.

LEVEL D - REMOTE. The level assigned when both a safety feature and approved procedures, or two independent safety features exist that collectively should prevent the Undesired Event from occurring.

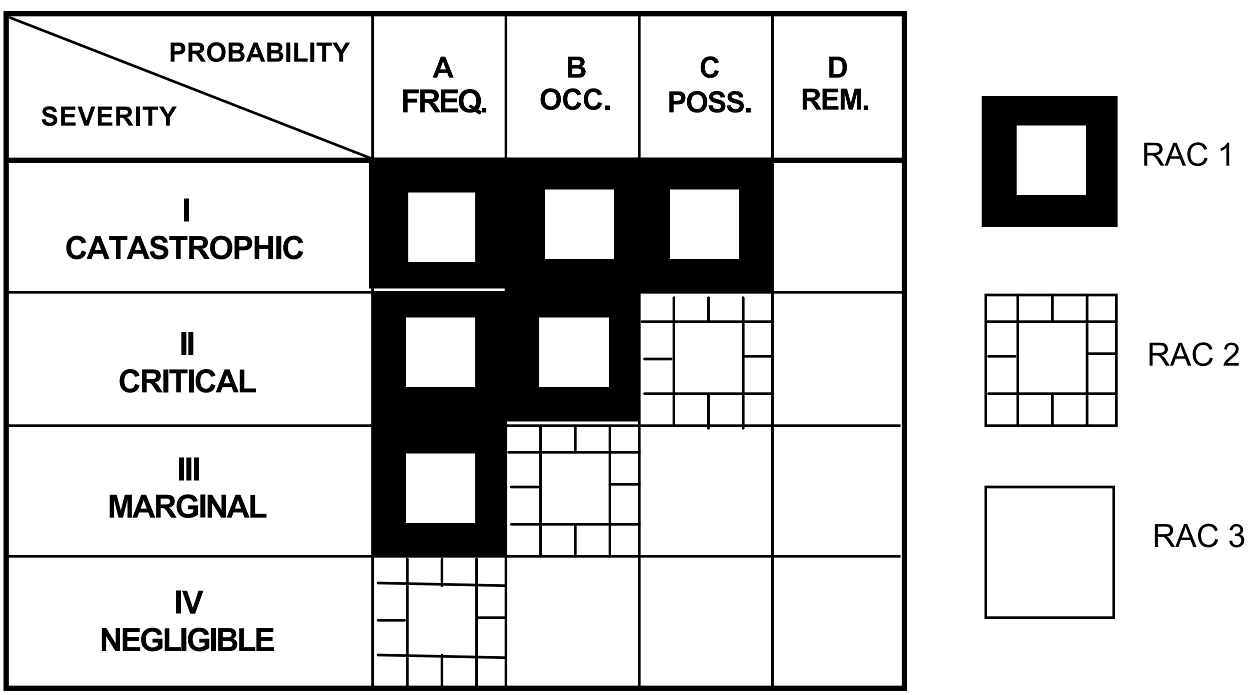

Figure 2-2, Risk Assessment Matrix.

2.4.4 Risk Assessment

An alphanumeric risk level, based on both Severity and Probability of Occurrence, shall be assigned to each Cause of an Undesired Event. The following paragraphs address how those risk levels are converted into a RAC using LaRC's risk matrix, which is depicted in Figure 2-2, "Risk Assessment Matrix."

2.4.4.1 Severity Category

A Severity shall be assigned to each Undesired Event assuming it will occur. In this analysis, the worst possible results is to be assumed with no consideration being given to abatement techniques incorporated in the system design or to the use of procedures. The Severity Category provides a relative measure of the worst possible consequences resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies, and subsystem or component failure/malfunction. The Severity Categories are:

- **Category I - Catastrophic** - May cause death, permanent disability, the hospitalization of three or more people, and/or system/equipment damage in excess of $250,000 (Type A or B Mishap).
- **Category II - Critical** - May cause lost time injury or illness, and/or system/equipment damage between $25,000 and $250,000 (Type C Mishap).
- **Category III - Marginal** - May cause minor injury or illness, and/or system/equipment damage between $1000 and $25,000 (Reportable Incident).
- **Category IV - Negligible** - Will not result in injury, illness, or system/equipment damage not in excess of $1000 (Non-Reportable Incident).

2.4.4.2 Probability of Occurrence Level

A Probability of Occurrence shall be assigned to each Cause of an Undesired Event. The Probability of Occurrence provides a measure of system safety by evaluating the system design in conjunction with abatement techniques, inspections, tests, and operating procedures. The Probability of Occurrence is the probability that a failure will occur sometime during the planned life of the system. The probability level shall be qualitatively based upon engineering judgment with appropriate guidelines. Those guidelines are:

- **Level A - Frequent** - The level assigned when neither a safety feature nor approved procedures exist to prevent the Undesired Event from occurring.
- **Level B - Occasional** - The level assigned when a safety feature does not exist, but the use of approved procedures should prevent the Undesired Event from occurring.
- **Level C - Possible** - The level assigned when approved procedures do not exist, but an existing safety feature should prevent the Undesired Event from occurring.

- **Level D - Remote** - The level assigned when both a safety feature and approved procedures, or two independent safety features, exist that collectively should prevent the Undesired Event from occurring.

2.4.4.3 Establishing a Risk Assessment Code (RAC)

First, the Effect of an Undesired Event is evaluated in terms of Severity (I, II, III, or IV). Next, the Probability of Occurrence (A, B, C, or D) is determined for each Cause of the Undesired Event. Using the severity of the Undesired Event, each cause is assigned its own unique alphanumeric Risk Level (for example, IA, IIB, IIIC, etc.). Finally, using the two-dimensional risk matrix, Figure 2-2, each risk level is translated into one of three Risk Assessment Codes (RAC's) - RAC 1, RAC 2, or RAC 3. They are pattern-coded on the matrix to distinguish each from the other. RAC 1's include blocks IA, IB, IC, IIA, IIB, and IIIA. RAC 2's include blocks IIC, IIIB, and IVA. All other blocks are RAC 3's.

2.4.4.4 Implications of a Given RAC

A RAC is a measure of the severity of an Undesired Event verses the probability that the event will occur. As such, its value has implication of what shall be done prior to operation of a facility.

RAC 1's are the most serious of the three levels of Risk Assessment. Accordingly, it is in the best interest of all concerned to eliminate them through redesign, safety devices, special operating procedures, or combinations of such methods. The implications of a RAC 1 shall be as listed below and depend on whether the FSSA is being conducted on a new facility, CoF Project, or existing facility.

- **New/CoF Project** - RAC 1's for new facilities, and those associated with a major Construction of Facilities (CoF) project in an existing facility, are of major safety concern and require resolution (reduction of the RAC from 1 downward to 2 or 3) before the facility can initiate/resume operations.
- **Existing** - RAC 1's for existing facilities not undergoing a major CoF are a major safety concern and require either (1) resolution (i.e., reduction of the RAC from 1 to a 2 or 3), (2) an abatement plan approved by the Safety Manager, or (3) approval by the Executive Safety Board (ESB) before the facility can resume operation. The abatement plan is to be developed by facility personnel and approved by the Safety Manager within 30 days of knowledge of the RAC 1. It must provide a clear and attainable solution to ultimately reducing the condition to a RAC 2 or RAC 3. Failure to meet one of these requirements could result in facility shutdown.

RAC 2's are the second most serious of the three levels of Risk Assessment. The implications of a RAC 2 shall be as listed below and depend on whether the FSSA is being conducted on a new facility, CoF Project, or existing facility.

- **New/CoF Project** - RAC 2's for new facilities and those associated with a major CoF in existing facilities are also of concern and require special attention. The

FSH of the facility in question, with Safety Manager concurrence, shall by letter, inform the Competency Manager who oversees the facility of the nature of the RAC 2 and request approval to conduct operations. Operations shall not begin in that facility until the Competency Manager, with the concurrence of the Safety Manager and Chairperson of the final design review board, has responded by letter authorizing such action.

- **Existing** - RAC 2's for existing facilities not undergoing a major CoF require no such approval. Acceptance of the risk is acknowledged by the OSFA Safety Engineer, Safety Manager, and FSH by signing the SAR. Plans and programs to correct existing RAC 2 UE's, as time and resources permit, are considered sound management practice.

RAC 3's are at a risk level that only needs to be accepted by the OSFA Safety Engineer, Safety Manager, and FSH. Acceptance of the risk associated with these undesired events is acknowledged by signing the SAR.

2.5 LaRC INTERLOCK PHILOSOPHY

In order to conduct business at LaRC, large power sources, pressurized gases, vacuums, hazardous materials, heavy machinery, and many other potentially dangerous conditions are present. The integration of safety into such an operation ensures the protection of the community, operating personnel, equipment, and the environment. LaRC's cornerstone strategy to achieve safety is its Interlock Philosophy, which is described below.

- A credible single order failure that can jeopardize personnel or major equipment requires an interlock or protective device to prevent its occurrence.
- A safety interlock or protective device must be independent of the failure mode and cannot be compromised by occurrence of the credible single order failure.
- When an independent safety interlock or device cannot be provided due to the utilization of a common component or path, then an independent component and/or path is necessary (for example, hardwired backup of a software safety interlock or device).
- The safety interlock or device, unless it is verified automatically during startup (as a permissive), shall be periodically verified for operation. Period of performance shall be established by the safety analysis and specified in the SAR.
- Safety interlocks and devices, either software or hardware, must be under configuration control at the project level both before and during shakedown. Commencing at the Operational Readiness Review (ORR), these safety interlocks and devices shall come under CM in accordance with Chapter 3 of this handbook. At no time shall software changes be made while the facility is on line (in operation).
- Forcing of safety interlocks or devices during facility operation (temporary changes to complete a run or troubleshoot a problem) must be in accordance with an approved procedure and have the permission of the FSH or a designated alternate.

- Failures of catastrophic proportions identified by the FSSA shall be assessed individually in the safety analysis and redundant safety interlocks or devices provided.

The above philosophy must be pursued regardless of the type of process control or complexity of the research facility. Several techniques can be used to achieve these aims to permit the necessary research to be accomplished. These techniques are discussed in the following paragraphs, in order of effectiveness, beginning with the most effective.

2.5.1 Design

The first line of safety is the initial design of a research facility. Safety and interlock policies must be of equal and simultaneous consideration with research aims in the initial design phase of a facility. It is at this point that the best and the most cost-effective safeguards can be incorporated into a system.

2.5.2 Engineered Safety Features

Once a facility is constructed, additional safety margins can be attained by ad hoc, engineered safety features. Such devices are an integral, permanent part of the facility and its routine operation. Like design features above, they are to be passive in nature and require no special action to cause them to be effective.

2.5.3 Safety Devices

Adjunct devices, such as goggles, hard hats, and safety bars, enhance safety. However, they require a conscious act on the part of the operator to become useful. Although they may appear cost effective, their effectiveness is moot if they are not employed.

2.5.4 Warning Devices

Visual and audible means to alert personnel to hazards are economical, but they are not barriers. Many of the techniques in the previous paragraphs are barriers. The term “barriers” implies that such devices prevent the occurrence of Undesired Events. Warning devices are effective only when personnel are aware of them in sufficient time to react; and do, in fact, react.

2.5.5 Procedures/Training

The introduction of the human element into a perfectly designed and controlled hardware system brings with it a potential for unexpected results. To ensure that the occurrences of operator errors are minimized, a thorough training program shall be written and verified (ref. LPR 1740.7, “Process Systems Certification Program” for more details). The process shall be controlled by SOP’s. If operator training and procedure compliance are to be completely effective in lowering the probability of an Undesired Event to an acceptable level, they must be coupled with some, if not all, of the foregoing abatement techniques.

2.6 CRITERIA FOR DESIGNATING DRAWINGS AS CCD's

The hazard analysis is a detailed analysis that identifies hazards and the appropriate controls. This ensures the facility is safe at the start of operation, but it does not ensure a safety review of future changes to a facility. This is accomplished by designating the appropriate documents as Configuration Control Documentation (CCD) and placing these documents in the Facility CM Program. CCD documents will include the SAR, the SOP's and/or Checklists, any pressure systems documents, and the key facility mechanical, weld, and electrical engineering drawings and schematics. The OSFA Safety Engineer, FSH, and TPE shall be responsible for designated a drawing as CCD. Any drawing that:

- Supports the conclusions of the safety analysis, and/or
- Useful for troubleshooting electrical systems,

are designated as CCD. Members of the Facility Team may include other drawings as CCD if desired. The Recertification and Configuration Management (R&CM) Contracting Officers' Technical Representative (COTR) shall have the responsibility for resolving any differences of opinion and making final decisions regarding the disposition of all drawings chosen for inclusion in the CM Program.

Chapter 3

3. FACILITY CONFIGURATION MANAGEMENT (CM) PROGRAM

3.1 PROGRAM SUMMARY

The LaRC Facility CM Program includes over 50 facilities as shown in Figure 1-1, “Effort Code Summary.” LaRC’s CM Program provides for the ability to:

- Record and maintain safety analysis documentation,
- Document and maintain standard operating procedures (SOP’s) for use by operating personnel,
- Ensure the Office of Safety and Facility Assurance (OSFA) reviews changes that affect safety, and
- Establish and maintain a baseline for designated systems (e.g., electrical systems) and the relevant configuration control documentation (e.g., drawings).

In addition, the Facility CM Program provides for risk reviews that consist of Annual CM Meetings, Procedure Demonstrations, and continual System Safety Engineering Analyses.

3.2 CHANGE CONTROL

The cornerstone of LaRC’s Facility CM Program is the Change Notification Sheet (CNS) process. Any change to facility hardware that affects safety, CCD drawings, a SAR and/or SOP’s shall be processed through the CNS process. Changes to pressure systems documents (PSD) shall also be processed using the CNS process. This process ensures notification of the change to the affected parties, verification that no protective measures have been degraded or defeated, and that no new hazards have been introduced.

The CNS process requires the Facility Coordinator (FC), the Facility Safety Head (FSH), the Facilities Configuration Coordinator (FCC), and the Safety Manager to approve a CNS prior to any hardware changes. A safety and/or third party review shall be conducted for all modifications except those that are strictly administrative in nature. All affected documents (e.g. SAR’s, SOP’s, checklists, drawings, etc.) are redlined prior to implementation of the change.

The CNS process shall be conducted in accordance with one of two Langley Management System (LMS) Center Procedures (CP) - LMS-CP-4710, “Configuration Management for Facilities” and LMS-CP-4890, “Construction and Change Assurance for High Risk Facilities.” LMS-CP-4710 shall be used for minor changes, such as replacing a high-pressure valve with an equivalent component or a change that does not effect safety. More complex changes, such as adding a new system or a change that impacts safety, shall be conducted in accordance with LMS-CP-4890. Additional information to determine which LMS process shall be used is provided in Section 3.4.

3.3 UPDATING AND DISTRIBUTING CCD

The R&CM COTR shall ensure that all CCD’s are updated by the R&CM Contractor in accordance with the redlined documents submitted with an approved CNS. Updating CCD’s shall not occur until after the changes proposed by the CNS have been completed. The R&CM COTR shall also ensure that updated CCD’s are distributed as outlined in this section.

For each CNS completed, a distribution package will be generated. The package includes a cover letter that includes the statement "this is a completion of CM update and delivery CCD revision package" and includes at least the following information: CNS Number, EC, Facility Name and Building number. Each updated CCD shall be included as enclosures to the package. The FSH shall receive a package that includes the enclosures marked "Working Master." Engineering Drawing Files (EDF) shall receive a package that includes the enclosures marked "Historical Copy". The cover letter without enclosures shall be sent to the FC and Safety Manager. The R&CM COTR shall ensure a copy of the cover letter is kept in the R&CM Contractor's files.

3.4 TYPES OF CHANGE

Modifications to facilities at LaRC under the CM Program can be one of four types:

- Administrative change,
- No safety impact,
- Safety impact and construction not required, and
- Safety impact and construction required.

The CNS process required depends upon which of these four types of changes is occurring. The four methods are discussed in the paragraphs that follow.

3.4.1 Administrative Change

Facility modifications that are simply administrative in nature and do not affect safety can be implemented without a CNS. An example of such changes is the replacement of a mechanical or electrical component with an equivalent component. A CNS shall be required to update Pressure Systems Documents (PSD’s) when like for like replacements are made in a high-pressure system, and the CNS process shall be conducted in accordance with LMS-CP-4710.

3.4.2 No Safety Impact

Changes that require updating CCD but are initiated as no safety impact shall be processed in accordance with LMS-CP-4710. Even though the CNS has been marked “safety not affected,” LMS-CP-4710 requires a safety review to ensure no safety impact.

3.4.3 Safety Impact

For those facility modifications that affect safety, the CNS process shall be conducted in accordance with LMS-CP-4890. The primary objective of this process is to ensure the appropriate safety analysis is conducted and that existing CCD documents are updated and, if required, new CCD documents are identified. There are two possible “paths” through this process. The path chosen depends if the change is being conducted in accordance with LAPD 7000.2, “Review Program for Langley Research Center (LaRC) Facility Projects,” or not. Changes that are governed by LAPD 7000.2 are conducted as outlined in Section 3.4.4.

For changes that are not governed by LAPD 7000.2, a CNS shall be initiated and submitted through the CMOL system. Affected redlined CCD documents supporting the change shall be appended to the CNS and the electronic package forwarded through the FSH to the Safety Manager. Prior to the Safety Manager’s approval, the OSFA Safety Engineer responsible for the facility shall conduct a safety analysis. After approval by the Safety Manager, the package shall be forwarded to the FCC for approval. When the change is completed, the final redlined "as built" documents and field verified drawings shall be submitted to the R&CM Contractor for document/drawing update.

3.4.4 Change Controlled by Design Review Process

This method is used for major modifications that are governed by LAPD 7000.2, "Review Program for Langley Research Center (LaRC) Facility Projects." For changes in this category, the information below pertains.

- Prior to the Preliminary Design Review (PDR) the TPE or the Work Package Manager/Construction Manager [WPM/CM], in coordination with the FSH and FC, shall ensure that the affected portions of all existing drawings, including interface drawings, impacted by the project are field verified (FV) and redlined to reflect the true configuration of the facility.
- At the PDR, the OSFA Safety Engineer shall report on the FV status of the above mentioned drawings and present the results of the safety analysis.
- Following the PDR, the OSFA Safety Engineer initiates a CNS that covers the project. This CNS shall identify all existing CCD drawings, or other documents, and any new drawings/documents that are to be CCD’s.
- Prior to the Critical Design Review (CDR), all existing and proposed CCD documents shall be redlined to accurately reflect the intended configuration of the facility. Also, the TPE shall have a Field Verification Plan to assure all CCD drawings are field verified prior to the Integrated System Review (ISR).
- At the ISR, the Safety Engineer shall attest that all drawings previously identified as CCD’s have been FV and present the results of the safety analysis.
- At the Operational Readiness Review (ORR), the Safety Engineer shall provide the final, approved redlined SAR and SOP’s. The TPE shall also provide a complete set of "as built" redlined drawings signed off and approved as FV.
- At the completion of the ORR, the above-mentioned redlined documents shall be forwarded to the R&CM Contractor for incorporation into the CM Program.

3.5 CONFIGURATION CONTROL DOCUMENTATION - DRAWINGS

This section describes several unique aspects of drawings incorporated into the CM Program and designated as CCD. Section 2.6 provides guidelines for which drawings should be placed under configuration control.

3.5.1 Drawing Field Verification

All engineering drawings currently in the CM Program shall be classified as either field verified (FV) or unverified. Additionally, no new drawing shall be brought into the CM program (i.e., designated as CCD) unless it is first FV.

The field verification process shall be a hands-on verification of the validity of the drawing conducted by facility, OSFA, Systems Engineering Competency (SEC), or contractor personnel. A drawing which has been FV shall display a "FIELD VERIFIED" statement authenticating that action. That statement shall be signed by the person attesting to the field verification. It shall also be signed and dated as approved by the Technical Project Engineer (TPE), FSH, or FC. If FV drawings are found discrepant, they shall lose their FV status and shall be identified as unverified. A sample of the FV statement is as shown below.

FACILITY BASELINE DRAWING
FIELD VERIFIED BY: ____________________
APPROVED BY: ____________________
LATEST DATE: ____________________

Drawings that are in the CM Program but are not FV shall display a "WARNING! UNVERIFIED" statement alerting the user that they are not field verified. A sample of that warning label is as shown below.

WARNING!
UNVERIFIED

All drawings that are currently in the CM Program and not FV are subject of an ongoing field verification effort by facility and SEC personnel as time and resources permit.

3.5.1 Changes to CCD Drawings

When drawings in the CM Program require change, the drawing shall be redlined. New items are added in green ink or in black ink highlighted in yellow marker. Existing items are deleted by marking over them in red ink. Redlined drawings shall be processed using the CNS process. The R&CM COTR shall ensure that the originals of CCD drawings are modified by the R&CM Contractor. The new original drawings are delivered to Engineering Drawing Files (EDF) and new WORKING MASTER copies are delivered to the facility.

3.5.2 Working Masters

For each CCD drawing, the facility shall be provided a current revision of the drawing marked “WORKING MASTER” in red ink. The intent of this procedure is to identify the drawing as a copy of the current configuration of the facility as described by the Master (reproducible) drawing. These WORKING MASTER drawings are to be kept in a central location at the facility and closely controlled to ensure availability to facility personnel.

In those cases where there are a number of CCD drawings which detail systems that affect more than one facility, each of the affected facilities will be listed, by EC, on the CCD sticker applied to the drawings. In addition, each of the affected facilities shall receive a new drawing marked WORKING MASTER in red ink. In this manner, each facility shall maintain a complete file of WORKING MASTER drawings that reflect the current configuration. With multiple copies of a WORKING MASTER, the situation can exist where one facility may have modified a system, including the redlining of the affected drawings, without informing the other facility having a WORKING MASTER of the same drawing. To preclude any adverse impact of changing a drawing with multiply ECs, the R&CM COTR shall ensure the R&CM Contractor coordinates the changes with the FSH of each EC.

Adherence to the following additional guidelines promotes accountability and use of WORKING MASTER drawings:

- A WORKING MASTER drawing shall always reflect the true ("as-built") configuration of the facility, which it represents.
- Proposed changes to a facility which impact a CCD drawing shall be redlined on a separate copy of the affected drawing, not on the WORKING MASTER.
- Changes, which reflect “as-built” configurations, shall be marked on the WORKING MASTER of each affected CCD drawing.
- The current WORKING MASTER (or a copy of it) shall always be present at the facility.

3.6 FACILITY BASELINE LIST (FBL) AND SUPPORTING FACILITY DOCUMENTS

A Facility Baseline List (FBL) can be generated for each facility in the CM Program using CMOL. The FBL represents a list of all CCD documents for the Facility. For those facilities that choose, a list of Supporting Facility Documents (SFD’s) will be maintained on CMOL. SFD’s are documents/drawings that are affiliated with the facility but not under CM control. It shall be the responsibility of the FSH or FC to update the list of SFD and submit any changes to the R&CM Contractor. SFD are not CCD’s, and their configuration is not maintained as part of the CM Program. Revision of SFD drawings is the responsibility of the facility since they are not CCD and are not updated by the R&CM Contractor.

3.7 FILING SYSTEMS FOR CCD's

The documents in the CM Program are stored as described in the following paragraphs.

3.7.1 Engineering Drawing Files (EDF)

EDF shall be the repository for all original (reproducible) configuration controlled drawings and for the microfilmed historical records of configuration controlled drawings and other CCD's. EDF will microfilm the original CCD's, and all subsequent changes, in order to create and preserve these historical records. Only the R&CM Contractor shall be permitted to withdraw CCD original drawings from EDF. Analyses, drawings, and nondestructive engineering information for systems that have been recertified or identified in the CIL shall also be stored in EDF.

3.7.2 R&CM Contractor Files

The R&CM COTR shall ensure that the R&CM Contractor maintains and stores the originals of all SOP's/Checklists, SAR's, and other CCD documentation. The originals of CCD drawings shall be stored at EDF. The R&CM COTR shall ensure the R&CM Contractor has on hand only those CCD original drawings that are being modified as directed by an approved CNS.

3.7.3 Facility Files

Each facility shall maintain its own filing system of current WORKING MASTER CCD's. Updates to these documents are provided by the R&CM Contractor, but the facilities must ensure that updates are posted and centrally stored so as to be of use when needed.

3.8 RISK AND CM REVIEW

The risk and CM review aspect of the CM Program consists of Annual CM Meetings, Procedure Demonstrations, and continual System Safety Engineering Analyses.

3.8.1 Annual CM Meetings

Annual CM Meetings shall be held for each LaRC facility in the CM Program to review facility documents and status, plans, and program effectiveness. These meetings shall be scheduled by the OSFA. Attendees include the FCC, FSH, FC, OSFA Safety Engineer, CM Engineer from the R&CM Contractor. OSFA shall issue a letter summarizing the meeting and delineating "action items." The minutes shall be permanently maintained by the R&CM contractor as documentation that the CMOL documents have been reviewed and re-approved.

3.8.2 Procedure Demonstrations

Procedure demonstrations shall be conducted annually by OSFA to verify existing procedures. The demonstrations shall be scheduled and conducted in a manner that ensures all procedures are reviewed and re-approved at least once every 5 years. The R&CM COTR shall ensure that the R&CM Contractor coordinates these procedure demonstrations and conducts a spot check of the facility drawings at each demo. At the completion of a procedure demonstration, a letter shall be distributed to all participants documenting which procedures were demonstrated and the CNS numbers associated with any required changes. This letter shall be generated and permanently maintained by the R&CM contractor as documentation that the demonstrated procedures have been reviewed and re-approved.

3.8.3 Continual System Safety Engineering Analyses

All configuration changes submitted by CNS are subject to a Systems Safety Engineering Analysis by the designated OSFA Safety Engineer or R&CM Contractor's Safety Analyst/Engineer. During this process, the CM documents (e.g. SAR's, SOP's, Checklists, D-6, engineering drawings) are analyzed to assess the safety impact of the proposed changes.

3.9 CONFIGURATION MANAGEMENT ON-LINE (CMOL)

Using LaRCNET, CCD's in the LaRC Facility System Safety Program are accessible electronically and the CNS process is implemented electronically. The R&CM COTR shall ensure that the day-to-day operation of this Configuration Management On-Line (CMOL) system is conducted by the R&CM Contractor. The CMOL system provides for searching and viewing CCD's and provides for electronic CNS processing (i.e., CNS Workflow).

3.9.1 Access and Database Maintenance

Access to CMOL shall be by authorized personnel, through LaRCNET, at "http://cmol.larc.nasa.gov." Entry into the CMOL system shall be controlled by use of a user name and password. The user name shall be the users first initial, middle initial, and the first six letters of the last name. Any employee can obtain access to CMOL by contacting the R&CM Contractor to request an account. However, the R&CM COTR shall approve any account that requires authority to approve a CNS.

The R&CM COTR shall ensure that the documents in the CMOL database are updated by the R&CM Contractor as they are revised. New documents shall be entered into the CMOL database within 10 working days of issuance. If there is a question concerning the currency of a particular document, call the R&CM Contractor for assistance and/or confirmation.

3.9.2 CNS Initiation/Processing

At the CMOL homepage, the user selects the "Proceed to CNS Workflow System" to initiate, approve, or view a CNS. The CNS workflow screen allows for three options from which to select. The first option allows the user to create a new CNS Work Package on line, and the second allows for searching for a particular CNS Work Package that is already in the system. The third option allows the user to status CNS Work Packages over which the user has authority or requires the users attention (i.e., review and approval). A users manual detailing this section of the CMOL system is accessible electronically from the CNS Workflow screen.

Chapter 4

4. PRESSURE SYSTEMS CONFIGURATION MANAGEMENT (PSCM)

4.1 PROGRAM SUMMARY

As part of LaRC's Pressure Systems Recertification Program, a Pressure Systems Document (PSD) is developed for ground-based high-pressure systems. For additional information about the Pressure Systems Recertification Program refer to LPR 1710.42, "Safety Program for Maintenance of Ground-Based Pressure Vessels and Pressurized Systems." The Pressure Systems Configuration Management (PSCM) program maintains the configuration control of all PSDs using the CNS process outlined in Chapter 3 of this document.

Any change, whether administrative in nature or not, to a high pressure system covered by LaRC's Recertification Program shall be documented using the CNS process. Changes that are administrative in nature, such as replacing a high-pressure valve with an equivalent component, shall be performed in accordance with LMS-CP-4710, "Configuration Management for Facilities." Other change shall be conducted in accordance with LMS-CP-4890, "Construction and Change Assurance for High Risk Facilities".

The R&CM COTR shall ensure that after a change has been approved and the work has been completed the R&CM Contractor field checks the changes and updates the affected CM documents. Any discrepancies found during the field check shall be appropriately redlined and reviewed by the Pressure Systems Engineer and the FSH prior to incorporation into the CCD.

4.2 PRESSURE SYSTEMS DOCUMENT (PSD)

The R&CM COTR shall ensure that PSD are produced by the R&CM Contractor for all ground-based high-pressure vessels/systems in accordance with LPR 1710.42, "Safety Program for Maintenance of Ground-Based Pressure Vessels and Pressurized Systems." The PSD is a compendium of component information and sketches and consists of:

- **Title Page** - Identifies the document as a PSD, the facility number and name, the system name and designation, and the PSCM document number.
- **PSCM Revision Record** – Reflects the approval of all issues of the PSCM.
- **Table of Contents**.
- **Introduction** - Discusses the development, purpose, and uses of PSCM.
- **Definition of Symbols**.
- **Key to Recertification Sheets** (Component Inventories).
- **System Description**.
- **Isometric Drawings**.
- **Recertification Status Sheets**.
- **Footnotes**.
- **Document Reference Sheet**.

Chapter 5

5. FACILITY SOFTWARE ASSURANCE AND CONFIGURATION MANAGEMENT

5.1 GENERAL

The use of automated control systems, for example programmable logic controllers (PLC) and PC's, by LaRC research facilities has generated the need for configuration control of software, including PLC logic. This chapter outlines the requirements for the Software Configuration Management (SCM) Program at LaRC research facilities.

5.2 PROGRAM OVERVIEW

The development/acquisition of software products for LaRC research facilities shall be in accordance with LMS-CP-5528, "Software Planning, Development, Acquisition, Maintenance, and Operation." The required level of configuration control during development shall be in accordance with LMS-CP-5528 and meet the requirements of LMS-CP-5529, "Software Configuration Management Planning for Low-, High-, and Critical-Control Software."

Each research facility using an automated control system that is responsible for performing safety functions (e.g., correct valve sequencing, shutdown the facility in an overtemperature condition) shall develop a Software Configuration Management Plan (SCMP). Programmable logic controller (PLC) logic is considered software for facilities that use a PLC to control facility systems and/or perform safety functions.

The SCMP shall be developed in accordance with LMS-CP-5529, and placed under configuration control in CMOL. In addition, the plan shall define a process to identify and review changes that directly affect safety prior to implementation. Changes that modify a hazard control (e.g., interlocks, valve sequencing) of an Undesired Event identified in the Safety Analysis Report (SAR) or affect the safety of the facility shall be processed using a Change Notification Sheet (CNS). This ensures a safety review by the FSH, the FC, an OSFA representative, and a SEC representative. The CNS also ensures other CCD documents (e.g., SAR) are updated as required. The Software Configuration Manager (SCM), who shall be defined in the SCMP, shall initiate the CNS. If the SCM has any question about the safety impact of a change, the FSH or an OSFA Safety Engineer shall be consulted.

For a facility with a SCMP developed prior to the first release of LMS-CP-5529, a new SCMP that meets the requirements of LMS-CP-5529 is not required until new software is developed/acquired. However, if the existing SCMP does not clearly define a process to review changes that impact safety, a new SCMP shall be developed.

Chapter 6

6. LABORATORY RISK EVALUATION PROGRAM (LREP)

6.1 PROGRAM SUMMARY

Over 120 pieces of research equipment, henceforth called Laboratories, are covered by the Laboratory Risk Evaluation Program (LREP). The program's objectives are:

- Establish a separate CM Program for NASA LaRC Laboratories which are not in the Facility CM Program or covered under Safety Permit,
- Increase safety awareness at those facilities at the operator level, and
- Enhance the capability of OSFA to monitor the safety aspects of Laboratory operations and assist in the resolution of unsafe practices.

The key elements of this program are two documents, Laboratory Risk Evaluations and Laboratory Operating Procedures, for each of the identified pieces of research equipment. These documents shall become CCD and be subject to CM as outlined in Section 6.4.

6.2 LABORATORY RISK EVALUATIONS (LRE's)

The term Laboratory Risk Evaluation (LRE) was established to identify the Safety Analysis efforts associated with the LREP. A LRE documents the hazard analysis performed on the laboratory. In most cases, the analysis is based on data from manufacturers' handbooks, discussions with operator and maintenance personnel, visual inspections, maintenance factors, and procedures. Management personnel shall take the steps necessary to correct any RAC 1 and/or RAC 2 Risk Assessments revealed in the documented Risk Evaluations (see Section 2.4.4).

An LRE consists of a Title Page, LREP Revision Record, Introduction, Laboratory Description, and Risk Evaluation developed as described below.

- **Title Page** – Identifies the document as an LREP product, states the name of the Laboratory, provides the facility number in which the Laboratory is located, and provides a unique document identifying number. The unique identifying number shall be a combination of the facility number and the order in which the LRE was completed for that facility, for example 1148-1, 1148-2, and so forth.
- **LREP Revision Record** – Reflects the approval signatures for the initial issue and all LRE changes at the direction of the approving authority.
- **Introduction** – Provides the purpose and philosophy of the analysis and explains the RAC logic.
- **Laboratory Description** – Gives a brief overview of the laboratory, lists major capabilities, and discusses the nature of research that can be conducted. This section may also include a Facility Block Diagram of the laboratory being evaluated.

- **Risk Evaluation** – Provides the complete assessment of the laboratory's operational environment. It includes general observations and general recommendations that address the existing conditions in a broad fashion.
- **Tabular Summary** - Column I enumerates each identified Hazard. In the second column, marked "Risk Evaluation," the analyst describes the Undesired Event, the potential causes and effects, what is presently in place to prevent its occurrence, and what other safety devices and/or procedures might further preclude the event. Following this, the analyst shall assign a Hazard Level, which is derived from the standard Risk Assessment Matrix discussed in Section 2.4.4, and included in each RE. This section also contains appropriate recommendations, which, if implemented, will reduce the assigned Hazard Levels.

6.3 LABORATORY OPERATING PROCEDURES (LOPS)

The first two pages of a Laboratory Operating Procedures (LOP), the Title Page and Revision Record, are identical to that of a LRE. The next page is a general opening page addressing the Purpose, Personnel, Support and Safety Services, and Initial Conditions appropriate to the procedures that follow. The procedures can be numbered in one continuous sequence or divided into Pre-Operational, Operational, and Post-Operational sections. The unique identifying number for procedures shall be derived simply by adding a “P" to the identifying number of the LRE which the procedures support (e.g., 1148-IP, 1148-2P).

6.4 LREP CHANGES AND DISTRIBUTION

LREP changes shall be initiated with a NASA Langley Form 129, "Change in Laboratory Equipment/Procedures (CLEP)." The final recipient of the CLEP form shall be the R&CM Contractor. The R&CM COTR shall ensure that the R&CM Contractor changes the original documents as outlined in the CLEP.

For each CLEP completed, a distribution package will be generated. The package will include a cover letter that includes the statement "this is a completion of CM update and delivery CCD revision package" and include at least the following information: CLEP Number, LREP Number, Facility Name and Building number. Each updated CCD shall be included as enclosures to the package. The FSH shall receive a package that includes the enclosures marked "Working Master." Engineering Drawing Files (EDF) shall receive a package that includes the enclosures marked "Historical Copy". The cover letter without enclosures shall be sent to the FC and Safety Manager. The R&CM COTR shall ensure a copy of the cover letter is keep in the R&CM Contractor's files.

Chapter 7

7. ASBESTOS CONFIGURATION MANAGEMENT

7.1 PROGRAM SUMMARY

The objectives of LaRC's Asbestos Safety and Configuration Management Programs are:

- Enable LaRC to comply with the myriad of clean air emission regulations established by the Environmental Protection Agency (EPA), the Occupational Safety and Health Administration (OSHA), and the Commonwealth of Virginia;
- Increase safety awareness and minimize the risk of asbestos exposure to personnel; and
- Institute controls to prevent the release of asbestos fibers, restrict future asbestos use, and develop surveillance and control of known, existing asbestos applications in LaRC facilities.

The safety requirements for asbestos removal are addressed in LPR 1740.2, "Facility Safety Requirements." In summary, prior to any operation involving removal and repair of known asbestos or any other procedure that may release airborne asbestos, an inspection must be performed by an inspection team. The team shall include an OSFA Industrial Hygienist (IH). In addition, operational and control procedures shall be documented, and prior to the start of operations, approved by the OSFA.

This chapter addresses the configuration management of known, existing asbestos applications in a facility. Over 250 LaRC facilities participate in this program. Each facility has been inspected to identify friable and nonfriable asbestos containing building material (ACBM) and written inspection reports were provided to the FSH's. These inspection reports were the baseline documents used to generate the Asbestos Configuration Management Reports (ACMR).

7.2 ASBESTOS CONFIGURATION MANAGEMENT REPORTS

An ACMR provides facility personnel, especially the FSH and FC, a document that identifies known asbestos applications. The report consists of:

- **Title Page** – Identifies the document as a configuration controlled document, identifies the facility by number and name, and identifies the current document revision.
- **Revision Record** – Reflects the approval signatures for the initial issue and all subsequent changes.
- **List of Page Revisions** – Enumerates each page in the document and the current revision letter of each page.
- **Introduction** – Provides the purpose and philosophy of the document.
- **Facility Asbestos Summary** – Describes in narrative form the asbestos status of the facility.

- **Facility Diagram** – Depicts the actual location of positive samples where asbestos is located in the facility.

7.3 ASBESTOS CM CHANGES

Upon completion of a Asbestos abatement project, the OSFA IH shall notify the R&CM Contractor that the project is complete. The R&CM COTR shall ensure that the R&CM Contractor incorporates the description of work and an updated Building Diagram into the facility ACMR. The revised ACMR shall be submitted to FSH for approval and distributed to the FSH, OSFA, and EDF.

Appendix A

A. GLOSSARY OF KEY TERMS

Asbestos CM Program (ACMP). A program designed to ensure NASA Langley Research Center (LaRC) compliance with asbestos-related EPA, OSHA, and Commonwealth of Virginia clean air emission regulations. This program generates and maintains current records of the location and status of all known asbestos at the Center.

Cause. The stimulus or triggering mechanism/act which precipitates an Undesired Event (accident).

Change in Laboratory Equipment/Procedures (CLEP) Form. NASA Langley Form 129 prepared by LaRC personnel and processed by contractor personnel. It is used in the Laboratory Risk Evaluation Program (LREP) to request approval of and record all changes made to the affected LREP equipment/procedures and its supporting CCD's.

Change Notification Sheet (CNS). NASA Langley Form 127, "Change Notification Sheet," prepared by LaRC personnel and processed by contractor personnel. The CNS action is processed electronically via the LaRC Configuration Management On-Line (CMOL) system. It is used in the LaRC Facility System Safety Program to request approval of and record all changes in the affected facility and to its supporting CCD's.

Checklist. An abbreviated set of written instructions for operating a facility. Checklists are derived from SOP's and contain sufficient detail to enable safe operations by the most experienced operator personnel. Checklists are developed and maintained under the CM Program.

Configuration Controlled Documents (CCD's). Those facility baseline documents that are considered critical to describing how a facility is configured, how it is to be operated, and what risks are associated with its operation. As such, CCD's are revised only through a formal change process under the CM Program. Examples of CCD's include, but are not limited to, Safety Analysis Reports (SAR's), SOP's and Checklists, certain Pressure System Documents (PSD's), and selected engineering drawings.

CM Update. The process of reviewing and documenting changes on a continuing basis. During this process, the reproducible masters (originals) of the affected documents are revised to incorporate the changes as shown on redlined documents. Revisions are initiated and tracked by the use of the CNS Form.

Configuration Management (CM). A discipline that establishes a baseline for facilities, selects technical and administrative documents, and exercises administrative control of all approved changes to that baseline.

Configuration Management On Line (CMOL). A LaRCNET-based server which enables users to access LaRC facility CCD's electronically via their desktop computer.

Critical Items List (CIL). A Critical Item is any item, the single order failure of which would likely result in death or damage to equipment or property equal to or greater than $1.0M. A CIL is a listing of such items for the affected facility.

Effect. The consequence of an Undesired Event/Accident in terms of equipment damage and/or personnel injury/death.

Effort Code (EC). A number that identifies a specific facility or group of facilities in the Facility CM Program. For the life of the facility, all CCD's will bear this number regardless of any facility name changes and/or hardware modifications.

Facility Baseline List (FBL). A list of all CCD documents that can be generated using CMOL.

Facility Configuration Coordinator (FCC). An individual appointed from the Systems Engineering Competency (SEC) who coordinates the support to the LaRC Facility System Safety Program. The FCC is also one of the approving officials for CNS's prior to any CM facility hardware changes which affect CCD documentation.

Facility Coordinator (FC) (see LAPD 1700.2, "Safety Assignments"). An individual appointed to coordinate the overall day-to-day operations of a LaRC facility. This individual uses assigned facility personnel, and additional support personnel as available, to accomplish the FC requirements listed in this handbook.

Facility Safety Head (FSH). An appointed individual who is responsible for providing the Facility Team direction, obtaining required support from knowledgeable research personnel, and approving all CCD's affecting the facility (see LAPD 1700.2).

Facility System Safety Analysis. A continuing analysis throughout all phases of the facility's life cycle involving the identification and control of hazards and the assessment of risks in operating that facility.

Facility Team. Personnel assigned to establish and prepare the Configuration Controlled Documents (CCD's) for a LaRC facility during the initial Systems Safety Analysis or any subsequent upgrade effort. The team is composed of the FSH, FC, FCC, Safety Manager, OSFA Safety Engineer assigned to the System Safety effort, and the CM (or other) contractor Safety Engineer.

Field Verified (or Field Verification). The process by which the accuracy of a CCD or any other drawing is verified. That accuracy is attested to by affixing a "Field Verified" statement, signed by the person doing the verification, and signed and dated by the Project Engineer, FSH, or FC.

Hazard. A condition which has the potential to result in damage to equipment and/or personnel injury/death.

Laboratory Risk Evaluation (LRE). A safety analysis completed under the authority of the Laboratory Risk Evaluation Program (LREP).

Laboratory Risk Evaluation Program (LREP). A program designed to provide Laboratory Risk Evaluations (LREs) and Laboratory Operating Procedures (LOP's) to selected laboratories at LaRC which are not in the CM Program and not covered with a Safety Permit.

Pressure Systems Configuration Management (PSCM) Program. A program to continuously update the In-service Inspection/Recertification effort.

R&CM Contractor. The R&CM Contractor is the Non-personal Services Contractor who supports the LaRC Facility CM Program.

R&CM COTR. The Contracting Officer's Technical Representative (COTR) for the R&CM contract.

Redlining. The process of identifying changes on facility documentation by making color-coded annotations on the documents themselves. Deletions to be made are lined through with red markings; additions are shown in green ink, or in black ink with yellow highlighting. Redlining of drawings may indicate proposed changes, or changes to show the "as is" condition.

Research Facility (Facility). A ground-based apparatus or equipment directly associated with research operations, and sufficiently complex or hazardous to warrant special safety analysis and control.

Safety Analysis Report (SAR). A report under the control of the CM Program which documents the formal Facility System Safety Analysis of a particular research facility.

Safety Engineer. A representative of OSFA, OSMA, or a support contractor who performs an initial Facility System Safety Analysis, and/or an upgrade of an existing one, and supports the CM activity for a particular facility.

Safety Manager, OSFA, OSMA. This individual reviews and approves all System Safety Analyses and reviews all changes to the SAR's, SOP's, and Checklists under the CM Program.

Single Point Failure. A discrete system element and/or interface, the malfunction and/or failure of which, taken individually, would cause failure of the entire system.

Standard Operating Procedures (SOP's). Detailed, written, step-by-step instructions to be routinely followed in operating a facility. SOP's contain all of the information considered pertinent to safe and efficient operation of the facility. SOP's are the source documents for Operational Checklists and are the basis, in part, for the facility Hazard Control Analysis. SOP's may also be used for training operator personnel. SOP's are under the control of the CM Program.

Supporting Facility Documents (SFD's). Those documents identified on the SFD list that are considered as part of the baseline documentation, but do not meet the criteria for CCD's.

Technical Project Engineer (TPE). The engineer assigned by SEC to manage repairs, rework, or modifications to an existing research facility or construction of a new facility.

Undesired Event. An event (or series of events) which unleashes the potential inherent in a hazard and, either directly or indirectly, results in damage and/or personnel injury/death.

Undesired Events List. A listing in the SAR of system failures/malfunctions derived from the preliminary hazard analysis that could, if not adequately controlled, result in personnel injury, unacceptable equipment/facility damage, and/or loss of productivity.

Working Masters. Copies of the latest-revision CCD's (SAR's, SOP's, drawings, and so forth) which are stamped "WORKING MASTER" in red and kept at the facility.

Appendix B

B. ACRONYMS

ACBM	asbestos containing building material
ACMP	Asbestos Configuration Management Program
ACMR	Asbestos Configuration Management Reports
CCD	Configuration controlled documentation
CDR	Critical Design Review
CIL	Critical Items List
CLEP	Change in Laboratory Equipment/Procedures
CM	Configuration Management
CMOL	Configuration Management On-Line
CNS	Change Notification Sheet
EC	Effort Code
EDF	Engineering drawing files
EPA	Environmental Protection Agency
FBL	Facility Baseline List
FC	Facility Coordinator
FCC	Facilities Configuration Coordinator
FSH	Organizational Facility Safety Head
FSSA	Facility Systems Safety Analysis
FV	Field Verified
HA	Detailed Hazard Analysis
ISR	Integrated System Review
LOP	Laboratory Operating Procedures
LRE	Laboratory Risk Evaluation
LREP	Laboratory Risk Evaluation Program
OP	Operational Procedures
ORR	Operational Readiness Review
PHA	Preliminary Hazard Analysis
PLC	Programmable Logic Controllers
PO	Post-Operational Procedures
PR	Pre-Operational Procedures
PSCM	Pressure Systems Configuration Management
PSD	Pressure Systems Document
R&CM	Recertification and Configuration Management
RAC	Risk Assessment Code
SAR	Safety Analysis Report
SCM	Software Configuration Management
SCMP	Software Configuration Management Plan
SCR	Software Change Request
SFD	Supporting Facility Documents
SOP	Standard Operating Procedures
TPE	Technical Project Engineer
WPM/CM	Work Package Manager/Construction Manager